REMARKS

Claims 1-9 and 13-20 are pending in the application. Claims 1, 9 (amended) and 13 are amended in order to better define the invention. Claims 10-12 are canceled without prejudice or disclaimer.

In a first examination report of the corresponding European Application, a reference to Chapter 3 of a book Electronic Payment Systems, Mahoney (Artech House, 1997) was provided. Applicants respectfully submit that the claims are distinguishable over the Mahoney text for at least the following reasons.

The present invention, as defined by claim 1 (amended), employs symmetric key encryption and public/private key operation to be used in combination. This is, in fact, a rather unusual combination since public/private key operation is essential for creating digital signatures that offer the non-repudiation characteristic similar to a human signature, while symmetric key encryption does not provide such a characteristic. On the other hand, symmetric key encryption is instead generally employed in cases when computational power is limited, such that public/private key operation is inapplicable. Consequently, symmetric key capable tokens (e.g. smart card) are widely available as low cost devices to achieve highly secure token-bond authentication/encryption, while public key based tokens are generally too expensive to be used in practical applications.

Despite this, the present invention, as defined by claim 1 (amended), is based on the realization that a high secure digital signature scheme can be provided using symmetric key encryption supported within a token at low computation cost, in combination with public/private key operation which can be performed on a computer terminal. The present invention thus makes highly secure transaction possible using a token which only supports symmetric key encryption, and which never outputs the symmetric key.

This application is completely different from the applications mentioned in Mahoney, for example, at pages 28-32, which deal exclusively with symmetric encryption, and principally with authentication rather than providing digital signature to a digital transaction. There is no discussion of the use of symmetric encryption and public/private key operation in combination, which reinforces the point made above that one skilled in the art regards these two cryptographic techniques as being largely mutually exclusive. This is clear also from the fact that the

discussion of public/private key encryption starting on page 33 of the reference is separate from the description of symmetric key encryption.

While there is a reference in section 3.6 of the document on page 35 to a combination of public key encryption and symmetric key encryption (see figure 3.13), the method is only for data encryption and is not relevant to the purpose of generating digital signature. Specifically, the system shown in figure 3.13 relates to encoding a message for confidentiality, and not to providing a digital signature. This is why figure 3.13 shows the public key encryption being performed using the recipient's public key and no the sender's private key as required by claim 1 (amended). Figure 3.12, by contrast, only shows the use of private key encryption, and symmetric key encryption is not employed at all.

The present invention, by contrast, requires that the use of data is encrypted first by a symmetric key operation, and then by a private key signature operation. Such a dual encoding is not suggested by the prior art at any stage, but is used by the present invention since it permits the on-token and off-token operations to be separated. There is no mention in the Mahoney reference of the technical situation addressed the present invention (that is a token which is incapable of public/private key encryption used in combination with another unit which is capable of public/private key encryption), and therefore Mahoney provides no teaching which would lead to the present invention.

For these reasons, claim 1 (amended) is patentable and unobvious with respect to the teachings in Mahoney. Applicant looks forward to receiving a favorable examination which concludes that the presently claimed invention is patentable over the prior art.

Respectfully submitted,

SUGHRUE MION, PLLC
Telephone: (202) 293-7060
Facsimile: (202) 293-7860

WASHINGTON OFFICE

23373
PATENT TRADEMARK OFFICE

Alan J. Kasper
Registration No. 25,426

Date: December 13, 2002

APPENDIX

VERSION WITH MARKINGS TO SHOW CHANGES MADE

IN THE CLAIMS:

The claims are amended as follows:

1. (Amended) A method of ~~encryption for creating token bound output data from user data using a symmetric key capable token~~ generating a private key signature in respect of user data using a token, the token having stored therein a private key and a symmetric key, said method comprising the steps of

a. providing the user data or a representation thereof as an input to a symmetric key operation supported by the token,

b. retrieving the output of the symmetric key operation as the token signature; and

c. combining the token signature with the user data or representation to generate the token bound output data; and

d. providing the output data as an input parameter to a private key signature generation operation, to form a private key signature for the user data.

9. (Amended) A method as claimed in claim 1 wherein the ~~output data is used as an input parameter to a private key signature generation operations, to form a private key signature for the user data~~ token signature and private key are output from the token to a computer terminal whish uses the private key to perform the private key signature generation operation.

13. (Amended) A method of verifying a private key signature generated by the method of claim ~~12~~ 1 comprising the steps of using a signature verification operation to verify the token bound output data and re-generating the token signature using the symmetric key to verify the token.

Claims 10-12 are canceled.